Missouri Department of Natural Resources
Data Processing Policy

Topic:	Internet Acceptable Use
Item:	2
Status:	Version 1.1
Updated:	November 8, 2000
See also:	Administrative Policy 0030, Administrative Policy 5060, 1 CSR 20-3.070 Personnel Advisory Board Rules and Regulations

This Data Processing Policy
reviewed and approved

by: ***Original signed by Jeff Staake***
Jeff Staake, Dept. Deputy Director
Missouri Dept. of Natural Resources

on: **August 16, 2001**
Date

Introduction:

Internet use is intended to further the mission, goals, and objectives of the department; and can provide staff with a valuable tool to make their work more efficient and effective when used wisely. This policy is intended to ensure that all department Internet users understand their responsibilities and proper uses for the Internet.

Policy:

Internet access is for department business only. No other use of the Internet is allowed or is appropriate when using department time and/or resources. Most questions that staff have asked about what is or isn't appropriate come down to this very simple distinction.

Even when using the Internet for department business, there are other provisions that must be observed. See the following pages for further guidance on such issues, which are categorized for easier reference.

Individuals should discuss any questions related to this policy with their supervisor.

The department provides an internal e-mail system for staff use. Use of other e-mail and similar services is prohibited. This prohibition includes "Web-based" e-mail services, and other Internet services which offer interaction that could be handled via the standard departmental e-mail system.

Disciplinary Action:

An employee determined to be in violation of this policy is subject to disciplinary action, including dismissal, in accordance with *Administrative Policy 5060 - "Progressive Discipline",* and *1 CSR 20-3.070 of the Personnel Advisory Board Rules and Regulations*. Depending upon the circumstances of the behavior, an individual may also be subject to prosecution under State or Federal law.

Provisions for Retrieving and Transmitting Information:

A. Internet users are responsible for all material received under their account, including mail, data, documents, and software.

B. Internet users are responsible for the protection of all copyrighted materials received through the Internet to include dissemination, re-publication, or distribution of such materials.

C. Internet users are responsible for assuring that inappropriate materials including pornography and files dangerous to the department's network are neither accessed using the Internet nor transferred between department computers and the Internet. All files downloaded from the Internet must be checked for computer viruses before they are used. This includes files attached to e-mail messages.

D. Internet users will use discretion when downloading or uploading large files and databases which could severely hinder Internet access for other staff by exceeding available capacity. Questions about specific situations should be referred to the appropriate Information Resource Manager (IRM) or the MIS Help Desk.

Provisions for Publishing and Posting:

E. Internet users will not publish or distribute information using any Internet service besides electronic mail without the approval of their Program Director.

F. All information disseminated to the public through the Internet must be authored in accordance with department guidelines pertaining to the release of public information. Such information must always be directly related to the official duties and responsibilities of the department.

G. Internet users must not use the Internet for advertising, commercial ventures, political purposes, chain letters, or other inappropriate purposes. Even the appearance of impropriety or a misuse of state resources is unacceptable when communicating via a global computer network.

H. Internet users will keep their language within proper decorum. Profanity, obscenities, hate mail, harassment, discriminatory remarks, and other inappropriate language are prohibited.

Provisions for Security:

I. Passwords must be protected and not shared with or divulged to others. This helps ensure that data integrity and security are preserved.

J. Internet users will respect the rights and privileges of other users by not modifying files, data, passwords, or other information belonging to other users.

K. Internet users will not attempt to violate the integrity or security of the department's computer network nor those computing systems they access through the Internet. There are also State and Federal laws that criminalize such activities.

L. Internet users must realize that information placed onto the Internet can potentially be intercepted or monitored by individuals worldwide. Care must be taken to avoid transmitting information that would be embarrassing to or have negative consequences for the department or the individual. Information can similarly be collected on all Internet locations that users visit. Personal and confidential information in particular must not be posted on the

Internet, and transmission of such information via the Internet is discouraged unless reasonable security methods are used to protect confidential information.

M. Internet users must not use dial-up or similar technologies that connect to the Internet or other TCP/IP-based services (personal or department-provided) while their computer is also directly connected to the Internet via the department's firewall. Having two different Internet-type connections available on the same machine simultaneously exposes the department's and the state's internal networks to the potential of outside attack. Simply logging out of the department's network before using such a connection is not a solution; The hardware connection to the network must be disconnected before using such dial-up services. Contact your Information Resource Manager (IRM) or the MIS Help Desk for assistance in determining whether using a particular dial-up or similar service would violate this provision.

Provisions for Administration:

N. Internet users are responsible for reporting violations of this Acceptable Use Policy to their supervisor or the department's Ethics Ombudsman. *Refer to Administrative Policy 0030 - "DNR Ethics Ombudsman" for details on this position.*

O. Internet users must abide by existing state and federal laws regarding communications when using the system.

P. Internet users must ensure that time spent using the Internet, including time spent searching for information, is likely to have sufficient benefit to the department to justify the time spent. If searching the Internet for particular information becomes too time-consuming, other avenues should be considered.

Q. Internet users may not subscribe to pay Internet services that will be billed to the department without prior approval. DPSRs for such services should be clearly identified with the words "Internet service request", and indicate the type and length of service. Detailed justification may also be attached, and could expedite the approval process. Requests should be routed first to the appropriate Program Director, then the appropriate Data Processing Coordinator, and finally to MIS for approval. Other existing purchasing procedures must also be followed.

R. When Internet users are provided direct Internet access through the department's network, any existing Internet services on their computer such as dial-up accounts must be immediately disconnected and remain disconnected. (Portable computers that have dial-up needs outside the office are exceptions, provided that provision M is observed to protect network security.) *Refer to provision M for more*. If a computer has no other dial-up needs, it is strongly recommended that the dial-up software be removed or disabled, the phone line be unplugged from the computer, and that the phone service be disconnected if there is no other use for that line.

S. Prospective Internet users must coordinate with their supervisor on what, if any, Internet usage is appropriate to their job function. Such determinations are ultimately at the discretion of their Program Director.

T. Many common Internet services including Web access will be enabled via the department's network by default. Less common services will be blocked by the department's firewall to enhance security. Requests to enable additional services should be routed first to the appropriate Program Director, then the appropriate Data Processing Coordinator, and finally to MIS for approval. Including justification with such requests may expedite the review process.

U. In order to ensure that staff have an opportunity to see any important new information available on the department's Intranet, all department computers must be set to use the standard home page of: http://www.dnr.state.mo.us/default